verdantix

Smart Buildings

Green Quadrant: Integrated Smart Building Security Software 2023

By Sandy Rogers
With Rodolphe d'Arjuzon and Joy Trinquet

March 2023

This version of the report contains Verdantix's summary of Honeywell's offerings to help prospective customers evaluate whether the vendor is a good fit for their requirements. It does not contain other vendor profiles.

Smart Buildings

Green Quadrant: Integrated Smart Building Security Software 2023

By Sandy Rogers
With Rodolphe d'Arjuzon and Joy Trinquet

March 2023

Verdantix research indicates that corporate real estate and facilities management executives seek more integrated solutions to provide trusted building and security operations and to better protect the safety and wellbeing of their constituents. Digital advancements are paving the way for more flexible systems to provide both integrated and targeted operational views, automated workflows, deeper analytics and broader value propositions. This report provides a detailed, fact-based comparison of 10 prominent security software vendors in the market. Based on the proprietary Verdantix Green Quadrant methodology, our analysis comprised vendor briefings and product demos, customer and desktop research, and vendor responses to an in-depth 113-point questionnaire covering 11 primary capability and nine market momentum categories. Among the providers featured in the Leaders' Quadrant, five firms — Genetec, Siemens, Johnson Controls (JCI), Honeywell and Everbridge — demonstrated the most advanced unified security management capabilities.

Table of contents

Table of figures

Organizations mentioned

3xLOGIC, ABB, Access IS, acre security (ACRE), ActivIdentity, ALCEA, Allegion, AllGoVision, Allied Universal, Alphatron Security Systems, AMAG Technology, Amazon Web Services (AWS), American Dynamics, Aritech, Assa Abloy, Ava Security, Avigilon, Axis Communications, Bentel, Bluefield Smart Access, Bosch, BriefCam, Brightly Software, Brivo, Calipsa, Canon, Carrier Global, CEM Systems, CISA, Clay Solutions, Cloudvue, Cognimatics, Cognitec, Comfy, ComNet, Control ID, Crossmatch, Dahua Technology, Delta Controls, DSC, DW Spectrum, Eagle Eye Networks, EasyLobby, EcoDomus, Enlighted, Envision Intelligent Solutions, Envysion, Esotec, Everbridge, Exacq Technologies, Feenics, Fire Sentry Corporation, FLIR, FogHorn, G4S, Gallagher, Geoffrey Industries, Genetec, GE Security, Geutebrück, HID Global, Hikvision, Honeywell, IDEMIA, IdenTrust, Illustra, Inaxsys, IndigoVision, Ingersoll Rand Security Technologies, Innometriks, Interflex+, Interlogix, Ipsotek, ISONAS Security Systems, Johnson Controls (JCI), Kantech, LCN, LenelS2, Lumidigm, Matrix Systems, Mercury Security, Microsoft, Milestone Systems, Motorola Solutions, Nox Systems, Nx Witness, Onity, Open Options, Openpath Security, PACOM Systems, Pelco, Phoenix Systems & Service, Proteus, PTI Security Systems, Qognify, Qolsys, Quantum Secure, Ramdor, Rave Mobile Safety, Raytheon Technologies, Razberi Technologies, RS2 Technologies, S2 Security, SALTO Systems, Schneider Electric, Securitas, Security Enhancement Systems (SES), ServiceNow, Siemens, SimonsVoss, SimplexGrinnell, Sine Group, Smartvue, Software House, Sonitrol, Stanley Black and Decker, Sur-Gard, Tempered Networks, Time Data Security (TDS), Touchcom, Trane, Transom Capital Group, Tridium, Triton Partners, Tyco International, United Technologies Corporation (UTC), US Digital Designs, US GSA (General Services Administration), Vanderbilt Industries, Videotec, Vigilant Solutions (VaaS International Holdings), Vindex Systems, Visonic, Von Duprin, Watch Guard, xMatters, Xtralis, Z-Wave.

The State Of The Integrated Smart Building Security Software Market

Elements of security and trust are being increasingly woven into the fabric of everyday life, protecting us, and enabling us to smoothly navigate activities and environments. Firms need to ensure their workers, building occupants and assets are safe from a variety of threats. Beyond criminal behaviours such as theft, active shooters and workplace violence, organizations need to be prepared for physical accidents, public health emergencies and climate-related incidents. Security teams must be able to rapidly detect and respond to critical events, and ideally prevent them from occurring. They also need to support distributed locations and workforces. Meanwhile, tenants and employees expect seamless access to a combination of building assets, amenities and digital services.

Facilities and business executives recognize that security operations are critical and that dated physical security infrastructure can pose tremendous risk. Historically, many organizations have approached security technology strategies in a conservative manner, to limit disruption, cost and the potential hazards of change. Given the perfect storm of increased threat vectors, changing occupant engagement patterns and available technical innovations, organizations are now taking stock and looking for more modern, extensible solutions. Integrated security is increasingly being recognized as a critical enabler and is playing a larger role within the broader connected enterprise and building landscape.

Integration And Intelligence Define The Future Of Security Software

Security solutions touch many stakeholders – security personnel, facilities managers, human resources (HR) and IT administrators, reception managers, as well as building occupants and visitors – with each having varied process and informational needs. Integrated smart building security software is designed to provide a common platform to support multiple aspects of security operations, such as surveillance, access control, and alarm and incident management. These solutions ideally present a holistic view of an environment for greater situational awareness and help operators be efficient and effective through targeted information and automation.

Given advancements in technical architectures, open standards and cloud computing, integrated security software solutions are becoming more viable and accessible. Today's security technologies can apply greater data intelligence and process automation and are being designed to more widely integrate with building systems, enterprise applications, communication platforms, and Internet of Things (IoT) and edge processing systems, as well as a host of point security and occupant experience solutions. However, while the trend for more open solutions will continue, there is still a complex web of proprietary technologies to consider.

This report provides a detailed assessment of 10 prominent integrated smart building security software providers and their product offerings, leveraging the Verdantix Green Quadrant methodology. We developed a detailed model of functional, technical and market capabilities for integrated security software by leveraging insights from customer and vendor studies, and performed analysis through a combination of vendor briefings and product demonstrations, an intensive vendor questionnaire, desk research, and feedback from users of security solutions.

Buyer questions answered by this study include:

- **What is the current state of the integrated security software market?**
- **How can integrated security software support my wider smart building strategy?**
- **How can I benchmark the capabilities of integrated security software offerings?**
- **Which integrated security software solutions will best match the requirements of my organization?**
- **What factors indicate that an integrated security software vendor is a reliable partner for the future?**

The Physical Security Market Is Engaged In A Monumental Shift To Embrace Digital Operations

The physical security market is taking advantage of digital innovation, to drive insights and streamline activities for smarter operations. Historically, buyers have approached security solutions in silos, implementing disparate software applications and a host of peripherals such as card readers, entrance gates and CCTV systems. The market landscape for security technology has evolved to more fully embrace IP-, web- and mobile-based computing, cloud deployment models, analytics, IoT and more integrated, and integratable, solution suites. Integrated security software vendors are:

- **Transitioning their solutions to more modern architectures.**
  Many vendors are reworking their solutions or have recently released newly architected systems, natively designed for cloud and edge computing. Some of these advances also address system performance and scalability. For example, Johnson Controls (JCI) is re-architecting its system using microservices and upgrading its applications with web-clients as part of its new C•CURE IQ offering. LenelS2 (Carrier) has gone through a complete refresh of its OnGuard solution suite, to offer web-based application functionality. Meanwhile, solutions such as Brivo's Access, Motorola's Alta (Openpath and Ava Security), and Schneider Electric's Access Expert, present solutions natively designed for the cloud.

- **Coalescing security with broader facilities and occupant activities.**
  Security vendors are expanding their solution sets to support a broader set of building management and tenant experience applications. Smart building technology conglomerates are at varied stages of advancing digital platforms and solution suites, such as Carrier's Abound, Honeywell's Forge, JCI's OpenBlue, Schneider Electric's EcoStruxure, and Siemens's Building X. These offerings are typically more open, cloud-based solutions and thus positioned to integrate a broader array of internal and external technical services for a variety of business needs – including security. Smart building digital platforms aim to provide users with the ability to assess and interact with building operations across multiple domains, such as HVAC, security and safety. These platforms are being designed to provide holistic views of building and asset conditions, with some utilizing digital twin technology. Beyond presenting data from existing systems such as access control and security alarm systems, some of these platforms incorporate newly designed applications, such as Siemens's Building X Security Manager offering. Meanwhile, Brivo, given its experience in the multi-family residential business, offers home automation solutions and is furthering the ability of its access control system to facilitate occupant experience applications.

- **Embracing a layered approach to deliver more unified views.**
  Integrated security software vendors have embraced various strategies to provide a 'single pane of glass' within their solutions. Providers such as Honeywell and Siemens offer command and control solutions to support global security operations centre (GSOC) environments. Everbridge has its physical security information management (PSIM)-oriented solution, which can provide a holistic view across multiple third-party security systems. Genetec has rolled out its Dashboarding functionality, and LenelS2 (Carrier) offers its Magic Monitor, for users to create customized screens. A sweet spot for some providers within the integrated security solution space, especially for those providing PSIM and broader integration capabilities, is in providing customers with an environment to which they can add new capabilities while leveraging existing investments. Smart building technology conglomerates are taking this a step further with their digital platforms.

- **Emphasizing occupant and operator usability and efficiency.**
  Security and access control solutions have become multifaceted, often creating complex application and portal interfaces for users to navigate. Some vendors are tackling usability as they redesign their solutions for the cloud or are streamlining activities for particular stakeholders with persona-based web and mobile applications. Faster incident response, communications, and collaboration between parties have become more critical activities for security teams to orchestrate. Some firms provide low or no-code tools to help organizations design custom workflows, to automatically trigger notifications or guide users through standard operating procedures (SOPs) and incident management steps. Examples include Everbridge's Critical Event Management (CEM), Genetec's Mission Control, Honeywell's Incident Workflow, and Motorola's Orchestrate and Ally Incident Management options.

- **Starting to incorporate AI-related technology.**
  Security solutions are starting to incorporate AI and machine learning (ML) algorithms to address analytical challenges of volume and timeliness, helping to filter out noise and quickly identify potential threats. AI-infused video analytics and computer vision are being used for surveillance purposes. For example, Bosch's Intelligent Video Analytics, Brivo's Snapshot, and Motorola's Appearance Search and Unusual Motion Detection offerings help with identification and forensics tasks. Alarm and event correlation homes in on common patterns and recognizes related events across varied planes. Security systems are also incorporating external data to facilitate risk intelligence activities, such as Everbridge's Global Risk Intelligence platform and JCI's Risk Insight offerings.

- **Slowly adapting the proprietary nature of their security technology.**
  Historically, the security arena has been rife with proprietary software and hardware dependencies. An access management software solution may only work with certain controllers or door hardware, or a video management system (VMS) solution may tout special analytical capabilities that are uniquely dependent on that same provider's cameras. Many vendors go to market emphasizing their complete, albeit somewhat closed, end-to-end solutions – often gleaning half or more of their security revenues from equipment. Implementors may prefer working with this acquisition model, as it can simplify training, installation and procurement processes; small and midsized businesses (SMBs), or greenfield situations where buyers are only just evolving to adopt automated IP-based solutions, may also find it attractive.

  Nevertheless, pressure has been mounting for providers to support more open constructs and supply customers with more choices in how they instrument and extend their overall security environments. Beyond offering basic application programming interfaces (APIs) and software development kits (SDKs) to aid integration and customizations, security software firms are increasingly supplying specific connectors to complementary – and even, at times, competitive – offerings, and are more broadly supporting standards such as ONVIF. However, cross-vendor integrations and APIs are not all created equal. Buyers must carefully assess which capabilities are uni- or bi-directional in nature, how diligent all parties are at maintaining their integrations, how well they can secure the overall environment, and whether additional licensing costs will be incurred.

- **Recognizing the need to support certain 'open' technology options.**
  A subset of access management solutions interoperate with, or use original equipment manufacturer (OEM) technologies, based on more 'open' access controllers, such as HID's Mercury Security controllers. Using Mercury-based equipment can theoretically allow organizations to switch software between those providers without needing to 'rip and replace' all their equipment – although a note of caution should be sounded as to how easily this can be accomplished, given each product's technical foundation and licensing terms. Another vendor, Milestone, supplies video surveillance technology which the industry has embraced in a somewhat similar fashion. Whether as a current requirement, or as part of a future supplier risk mitigation strategy, buyers and integrators are becoming increasingly aware of this option and are factoring it into their purchasing decisions and recommendations.

Security Software Providers Reshape Market Boundaries

Leading integrated security software vendors are expanding their technological and market footprints through organic development, technology partnerships and acquisitions. It is important for buyers to keep up with overall market movements, technology roadmaps and partner relationships. The more these systems become interwoven, the more dependencies should be tracked and opportunities for innovation discovered. Customers need to be aware that:

- **Mergers and acquisitions are driving market consolidation.**
  The physical security technology market over the past decade has seen significant vendor consolidation and accelerating acquisition activity (see **Figure 1**). Acquiring firms must typically support a complex web of product lines, as the software, and often proprietary hardware, tends to be long-lived. Some firms have become market aggregators, while others have made strategic technology buys to fold into their platform or moves to jumpstart their presence in a particular facet of the market, such as cloud. Key examples to note are ACRE's ongoing investments across the security domain, JCI's large acquisition-merger with Tyco and subsequent transactions, and Motorola's rapid escalation in video security through a volume of acquisitions.

Figure 1

Accelerating Security Market Consolidation: Example Vendor Market Transactions

Current Firm		
Allegion		
Firm Acquisition History	**Date**	**Background**
STANLEY Access Technologies	2022	Door systems and hardware (Note: Stanley Black and Decker split its security-related product lines between Stanley Access Technologies and Stanley Security. Stanley Access Technologies was sold to Allegion, and Stanley Security was sold to Securitas)
ISONAS Security Systems	2018	Cloud-based access control software and hardware
SimonsVoss	2015	Keyless door entry
Ingersoll Rand Security Technologies	2013	Access control software and hardware; door hardware (Note: Allegion spun off from Ingersoll Rand in 2013. Includes CISA, LCN, Schlage and Von Duprin)
Interflex+	2000	Access control software and hardware; workforce management

Current Firm		
Allied Universal		
Firm Acquisition History	**Date**	**Background**
G4S	2021	Security services (Note: Includes AMAG, Touchcom)
Phoenix Systems & Service	2020	Security systems integration

Current Firm		
Assa Abloy		
Firm Acquisition History	Date	Background
Control iD	2022	Access control hardware and software; time and attendance
ALCEA	2022	Access control, surveillance and intrusion hardware and software
HID Global	2000	Access control hardware and software; secure identiy (Note: Includes ActivIdentity, EasyLobby, Lumidigm, IdenTrust, Quantum Secure, Crossmatch, PTI Security Systems and Access IS)
Mercury Security	2017	Access control hardware (Note: Acquired from ACRE)

Current Firm		
Canon		
Firm Acquisition History	Date	Background
BriefCam	2018	Video analytics
Axis Communications	2015	Access control and video surveillance hardware and software
Cognimatics	2016	Video analytics (retail)
Milestone Systems	2014	Video surveillance hardware and software

Current Firm		
Carrier Global		
Firm Acquisition History	Date	Background
United Technologies Corporation (UTC)	2020	Aerospace and building systems products and services (Note: UTC merged with Raytheon to form Raytheon Technologies in 2019 and spun off Carrier with LenelS2 in 2020 to create Carrier Global. Includes Onity)
Lenel Systems	2005	Access control systems (Note: Merged with S2 Security in 2018 to become LenelS2)
S2 Security	2018	Access control and video management systems
GE Security	2010	Fire detection and security solutions (Note: Includes multiple acquisitions, including Aritech - global intrusion and video; and Interlogix - alarm and video mgt, which shut down in 2019, with tech support ending in 2021)

Current Firm		
Honeywell		
Firm Acquisition History	Date	Background
US Digital Designs	2022	Public safety communications
Sine Group	2020	Cloud-based visitor and contractor management
Xtralis	2016	Fire detection and control
Fire Sentry Corporation	2012	Fire detection and control

Current Firm

Johnson Controls

Firm Acquisition History	Date	Background
Tempered Networks	2022	Edge cyber security
FogHorn	2022	Edge intelligence
Envision Intelligent Solutions	2022	Remote monitoring and perimeter protection services
Vindex Systems	2022	Security systems integration services
Esotec	2021	Security systems integration and managed services
Qolsys	2020	Intrusion and smart home devices
Tyco International	2016	Security systems; access control; video surveillance; fire detection and control; intrusion; video security cameras (Note: Includes Software House, American Dynamics, Kantech, DSC, CEM Systems, Sur-Gard, Bentel, Innometriks, SimplexGrinnell, Illustra)
Security Enhancement Systems (SES)	2022	Mobile and keyless access control
Smartvue	2018	Cloud-based video surveillance systems
Exacq Technologies	2013	Video surveillance systems
Visonic	2011	Intrusion security (residential)

Current Firm

Motorola Solutions

Firm Acquisition History	Date	Background
Ava Security	2022	Cloud-based video management software and cameras
Calipsa	2022	Cloud-based video analytics
Rave Mobile Safety	2022	Mass Notification and Incident Management
Envysion	2021	Video security and analytics (retail and restaurants)
Openpath Security	2021	Cloud/mobile access control
IndigoVision	2020	Video surveillance
Pelco	2020	Video surveillance cameras (Note: Schneider Electric acquired Pelco in 2002, and sold it in 2019 to Transom Capital Group, prior to being acquired by Motorola in 2020)
Videotec	2022	Video surveillance cameras
WatchGuard	2019	Mobile video (public safety)
VaaS International Holdings	2019	Licence plate recognition (Note: Includes Vigilant Solutions)
Avigilon	2018	Access control and video surveillance systems and cameras

Current Firm		
SALTO Systems		
Firm Acquisition History	**Date**	**Background**
Bluefield Smart Access	2022	Cloud-based authentication
Cognitec	2022	Biometrics
Clay Solutions	2017	Cloud-based smart locks

Current Firm		
Securitas		
Firm Acquisition History	**Date**	**Background**
STANLEY Security	2022	Security systems and services (Note: Stanley Black and Decker split its security-related product lines between Stanley Access Technologies and Stanley Security. Stanley Access Technologies was sold to Allegion, and Stanley Security was sold to Securitas)
PACOM Systems	2018	Security systems (Note: PACOM changed its name from Securitas Systems Group in 2008)
3xLOGIC	2018	Access control and video surveillance hardware and software
Sonitrol	2008	Access control, video surveillance, and intrusion systems
Alphatron Security Systems	2018	Camera, access control and communication system services

Current Firm		
Triton Partners		
Firm Acquisition History	**Date**	**Background**
ACRE	2021	Access control and intrusion hardware and software
Vanderbilt Industries	2013	Access control and intrusion hardware and software (Note: Comprises access control company Geoffrey Industries and some access control and video products acquired from Ingersoll Rand)
Siemens Security Products	2015	Access control, video surveillance and intrusion hardware
Time Data Security (TDS)	2021	Cloud-based visitor management and access control software
Feenics	2021	Cloud-based access control
Matrix Systems	2021	Access control and video surveillance systems
RS2 Technologies	2019	Access control hardware and software
Open Options	2018	Access control hardware and software
ComNet	2016	Video networking
Razberi Technologies	2020	Video surveillance hardware and software

Note: Table is illustrative in nature and is not meant to be an exclusive or complete list of transactions.
Source: Verdantix analysis

- **Software providers are continuing to expand their portfolios of offerings.**
  There is a wealth of innovation constantly taking place across the broader security domain. To facilitate integration, solution providers support an array of standards and API interfaces. Advanced applications, from biometrics to gunshot detection, are more readily combined with broader security platforms. Integrated security software vendors themselves offer various add-on applications, such as licence plate recognition systems, as with Genetec and Motorola. Most of the access control vendors Verdantix studied provide visitor management applications, although some offer additional solutions, such as Honeywell's Sine, emanating from an acquisition. The use of IoT systems and sensors in conjunction with security systems is an important and growing phenomenon.

- **Licensing models can be highly complex to navigate.**
  Many of the integrated security software vendors we analysed for this study offer an array of solutions. Somewhat stifling is the overwhelming volume of options that some vendors sell and license as separate product add-ons and plug-ins – adding to overall cost structures. This can make it difficult to compare solutions and can add complexity to procurement activities. Charges to use APIs and integrate third-party solutions are areas buyers should also examine carefully. The level of customer pain is beginning to be noticed by some vendors, and they are making moves to simplify their licensing and pricing models. For example, Genetec recently aggregated pricing for many of its core Security Center applications into three primary tiers.

- **Integrators levy significant influence.**
  The business of physical security is highly dependent on a large, localized channel of implementors and integrators. Most security software vendors will only sell through, train and allow certified service partners to interact with their technical support teams. This is in part due to the level of skills needed to ensure their solutions are properly installed and maintained to code. These outfits and individuals influence buyer choice – and satisfaction – with security system implementations. Service partners favour certain security vendors' technologies, due to the level of commitment required alongside their business arrangements and channel protection programmes. They can also have a heavy hand in overall user experiences with the technologies. It is critical that firms select their integrator partner carefully, especially as security computing environments expand and the number and complexity of integrations increase.

- **Configuration tooling is an area that remains somewhat fragmented.**
  The heavy reliance on the integrator channel has also influenced the evolution of security software itself. Many security systems separate operator-oriented applications from configuration tools. This presumes that integrators are not only the primary individuals involved in delivering initial system set-ups but are also the ones responsible for implementing ongoing changes, such as creating workflows, integrations and customized views for their customers. These tools can present varied user interfaces (UIs) and demand different skill sets. Vendors should consider that a blend of integrators and end-users will increasingly need access to and work with these tools; and that the usability of these tools will need to evolve as cloud- and software-as-a-service (SaaS)-based solutions continue to gain traction.

- **Supply chain strategies are adapting for resiliency and transparency.**
  Recent supply chain issues, due to geo-political and sourcing trends, have impacted the availability of security equipment, prompting some buyers to look for technically compatible alternatives. Some organizations may wish to assess their future security infrastructure needs and weigh the benefits of using software that can leverage a broader array of technologies and more open, standardized products. Vendors are increasingly being pressured to provide greater transparency into software and hardware OEM relationships and manufacturer sourcing, especially given cyber security concerns. For example, both the US and UK governments have taken steps to ban the importation and use of products from firms such as Dahua and Hikvision. Some vendors, such as Honeywell, which previously relabelled or OEMed such products, have pulled those offerings from focused regions; firms such as Motorola, meanwhile, are reinforcing local manufacturing capacity for National Defense Authorization Act (NDAA)-compliant systems.

Buyers Desire More Flexible And Modern Security Solutions

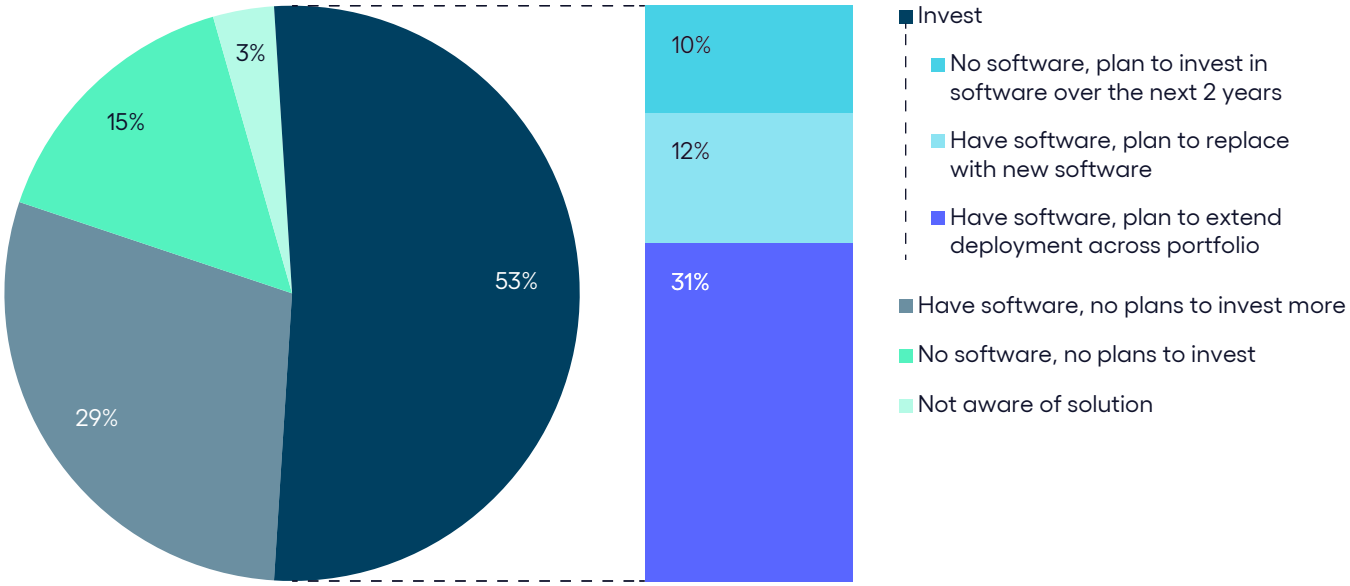
Organizations are taking stock of their capabilities to address changing security and safety demands. Rising security concerns, stress on resources and available skill sets, and changing occupant engagement preferences are driving businesses to seek more sophisticated and flexible security solutions. The COVID-19 pandemic and hybrid work patterns have accelerated the need for businesses to support remote security operations, provide touchless access options, and implement mobile credentials.

Security-related software investments are on the radar for many firms. According to our most recent global corporate smart building technology survey, more than half (53%) of the facilities and corporate real estate (CRE) executives studied plan to newly invest, replace or extend their deployments in physical access and security software (see **Figure 2**). For more information on this study, reference Verdantix Market Insight: Building Security and Safety Investment Trends 2022 and Verdantix Global Corporate Survey 2022: Smart Building Technology Budgets, Priorities & Preferences.

Figure 2

Current And Planned Investments In Physical Access And Security Software

To what extent do you use commercial software to support physical access and security?



Note. Data labels are rounded to zero decimal places.
Source: Verdantix Global Corporate Smart Building Technology Survey 2022

N=350

Organizations are looking for:

- **Modern security and access solutions to support changing demographics.**
  In today's digitally savvy world, employees and tenants expect consumer-grade technology experiences. Individuals increasingly desire self-service and mobile functionality to connect to spaces and services. Frictionless access is an ultimate goal. The Verdantix global corporate smart building study shows relatively strong interest in smart badges, biometrics and facial recognition, in addition to traditional access control and visitor management system investments (see **Figure 3**). Added considerations for aging populations include leveraging sensors for security and safety surveillance and modified access options.

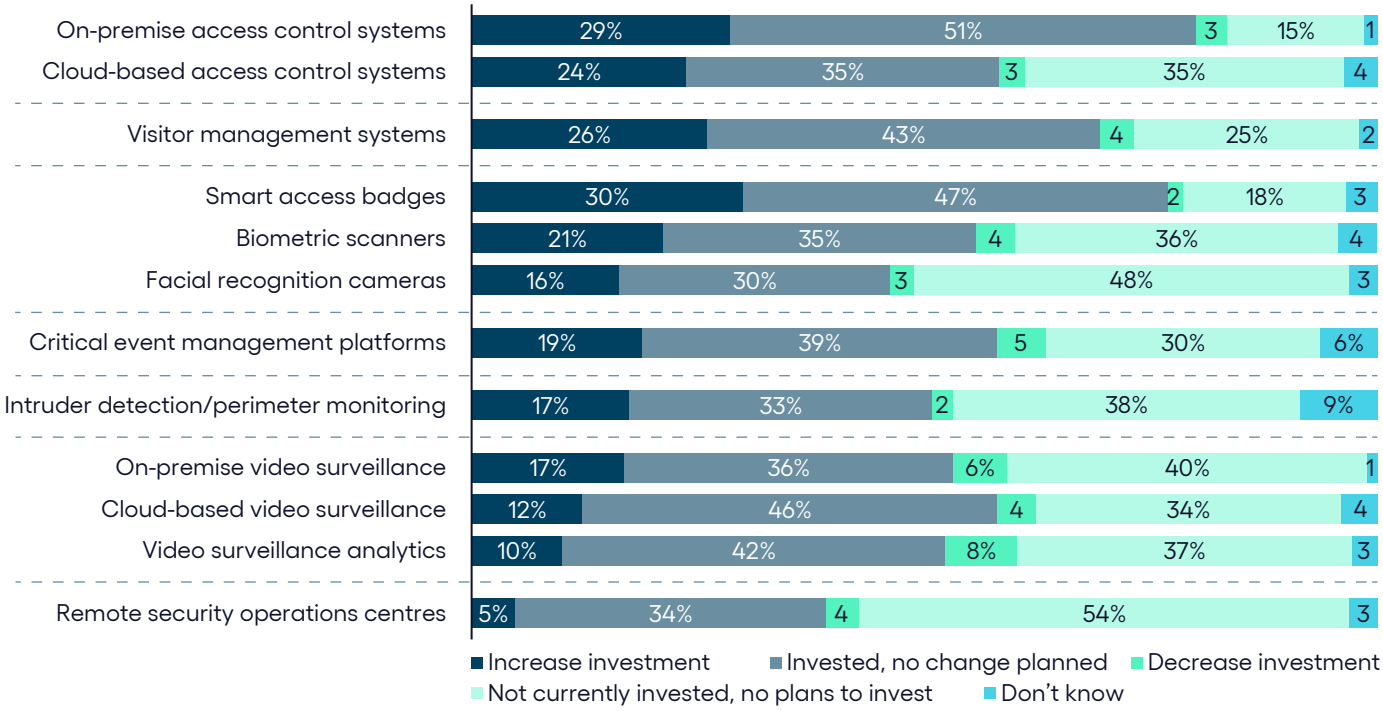
- **Security systems that enable seamless building and occupant experiences.**
  Security solutions are not only designed to protect individuals and assets; they are increasingly being used to help enterprises understand occupancy patterns and building conditions, and through credentialling provide tenant and worker access to amenities and environmental controls. Integrated smart building security software can interface with various communication systems for safety notifications or to provide occupants with guided instructions. These solutions can also ensure a smooth invite-to-gate-to-door visitor admittance process.

- **Scalable and extensible solutions to support distributed sites and workforces.**
  Large or growing enterprises seek assurances that their security infrastructure is flexible and resilient enough to adapt and scale as needed. Some organizations have found that when they reach a certain size, they need to shift security solutions to accommodate more complex access and security scenarios, or to support more users, access points, camera installations, or distributed sites. In addition, the ability to extend a given security software platform with additional applications, including third-party solutions, can be critical to particular types of businesses and industries.

Figure 3

Security Technology Category Investment Plans

What are your investment plans for the following building security solutions over the next 12 months?



Note. Data labels are rounded to zero decimal places; percentages less than 6% are written as numbers.
Source: Verdantix Global Corporate Smart Building Technology Survey 2022

N=350

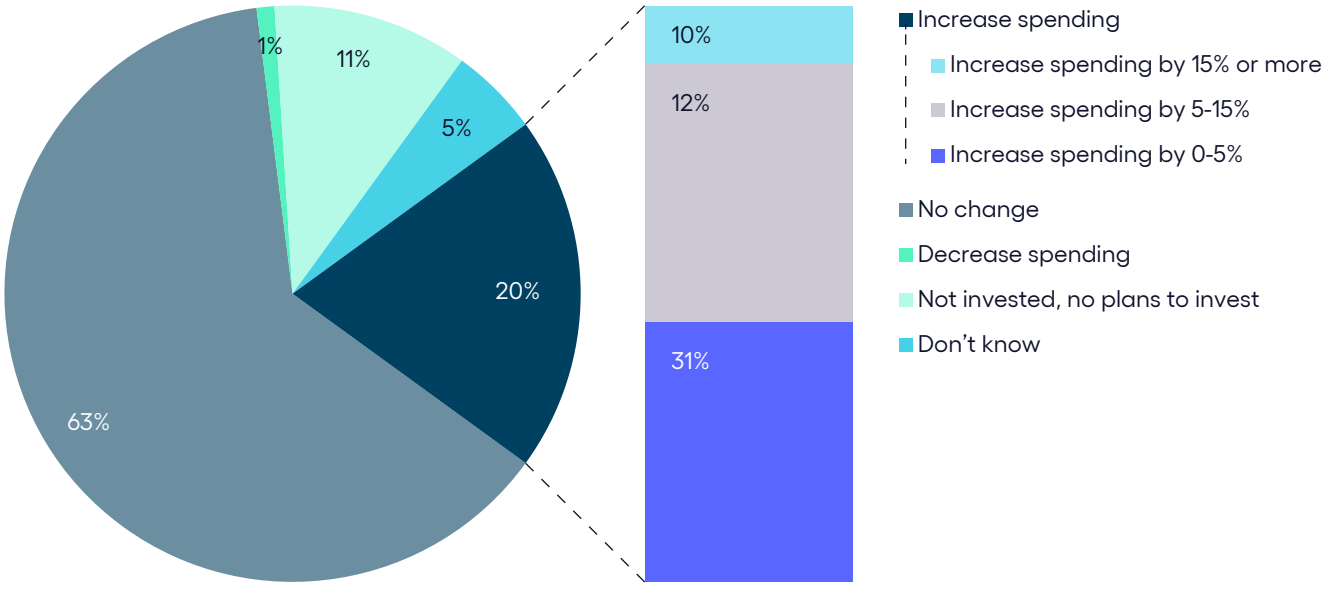
- **Cyber security and privacy assurances.**
  Security systems themselves can be vulnerable to attacks on both the IT and the operational technology (OT) front. While some organizations with sensitive environments are still hesitant to adopt cloud-based security systems, many are feeling more comfortable exploring these options. Surveillance systems and cameras, combined with edge computing architectures, are adding features to ensure individual privacy is retained. Vendors such as JCI and its Tempered Networks acquisition are incorporating greater network-based security protocols. The growing digital and IT-oriented trajectory of security systems presages the emergent alignment between physical and cyber security domains.

- **Intuitive, integrated security systems to address varied team skill sets.**
  Security operators, guards, administrators and facilities managers may all interact with varied aspects of security systems. It is imperative to supply these workers with systems that are easy to navigate, and ideally engage them in a proactive manner. Integrated security systems are designed to aggregate information and standardize access to subsystems, simplifying and streamlining the user experience. Embedded intelligence to automatically identify potential security threats and to filter alerts can save precious time, reduce manual activities and help assure critical events are not overlooked. Process and workflow automations can ensure proper procedures are followed and facilitate incident response. An increasing number of firms are recognizing the advantages of utilizing integrated security software with these valuable capabilities. Verdantix's global corporate smart building study shows that a fifth of the facilities and CRE executives surveyed have plans to increase spending on integrated building security platforms (see **Figure 4**).

Figure 4

Anticipated Spending For Integrated Building Security Platforms

Over the next 12 months, how do you expect your spending to change across the integrated building security platform software category?



Note. Data labels are rounded to zero decimal places.
Source: Verdantix Global Corporate Smart Building Technology Survey 2022

N=350

Green Quadrant For Integrated Smart Building Security Software 2023

Organizations and real estate executives are looking for increasingly intelligent solutions for more effective and efficient security and building operations, and positive occupant experiences. As such, the definition of integrated security is expanding, as is its role and context within the smart building space.

For the purposes of this report, Verdantix defines integrated smart building security software as:

> "Software designed to support the monitoring and management of the physical security of building assets and safety of occupants in a unified fashion."

The security technology landscape is broad and deep. This study looks at the intersection of multiple key facets of the delivery of physical security operations, such as centralized security management, access control management, surveillance management, event and alarm management, and visitor management.

It is important to note that this Green Quadrant analysis is designed to evaluate vendors with software platforms that support multiple aspects of security in a unified way. Integration capabilities, the ability of the software to provide a centralized view of the environment for situational awareness, and coordination of multiple stakeholder activities were key factors in our assessment. The study is not designed to assess security hardware, software as it specifically relates to security hardware performance, or professional service offerings.

Green Quadrant Methodology

The Verdantix Green Quadrant methodology provides buyers of specific products or services with a structured assessment of comparable offerings at a certain point in time. The methodology supports investment decisions by identifying potential vendors, structuring relevant purchase criteria through discussions with buyers and providing an evidence-based assessment of the products or services in the market. To ensure objectivity in the study results, the research process is guided by:

- **Transparent inclusion criteria.**
  We aim to analyse all providers that qualify for inclusion in this research. For those providers that declined our invitation or failed to respond, we worked to include them in the study based on whether we deemed it possible to provide an accurate analysis of their market positioning based on public information.
- **Analysis from the buyer's perspective.**
  We gathered input from security and facilities professionals to understand relevant buying criteria. This informed how we weighted the evaluation criteria in the model that drives the Green Quadrant analysis graphic. Additionally, we utilized data from Verdantix research and surveys of real estate and facilities management decision-makers to assess the evolving needs of customers.
- **Reliance on professional integrity.**
  As it is not feasible to check all data and claims made by vendors, we emphasize the need for professional integrity. Assertions made by software vendors are put in the public domain via this Verdantix report and can be checked by competitors and existing customers.
- **Scores founded on evidence.**
  To assess the expertise, resources, business results and strategies of individual providers, we collected evidence from public sources and conducted interviews with multiple spokespeople and industry experts. Where providers claimed to be 'best in class', we collated relevant evidence.

- **Comparison based on relative capabilities.**
  We construct measurement scales ranging from 'worst in class' to 'best in class' performance at a certain point in time. A provider's position in the market can change over time, depending on how its offering and success evolves relative to its competitors. A vendor's Quadrant positioning may not necessarily improve — even if it adds new capabilities, makes a strategic acquisition, or receives investment — as the assessment is relative to what other vendors are offering. The Green Quadrant analysis is typically repeated every one-and-a-half to two years.

Evaluated Firms And Selection Criteria

Verdantix defined vendor inclusion criteria to ensure that the Green Quadrant analysis compared firms providing similar offerings. The ten providers included in this study were selected because they have:

- **Ability to unify the five functional security categories evaluated in this study.**
  Reflecting growing market demand for more interconnected security solutions, to qualify for this benchmark study, the vendors included in the study are able to support the following security functions in a unified way: 1) centralized security management; 2) physical access control management; 3) visitor management; 4) surveillance management; and 5) event and alarm management.
- **Capabilities to support multi-site environments and at least 25 enterprise-scale security software customers.**
  We focused the study on vendors with the ability to meet the needs of diverse customers, including those operating in large-scale environments. For inclusion in this study, security software must be able to support sizable enterprise operations, including multi-site configurations.
- **An established partner ecosystem in the building security market.**
  It is imperative that today's security systems are adaptable and can participate in the broader context of an organization's operating and computing landscape. To qualify for this study, vendors needed to showcase their ability to integrate and fit within the wider security and smart building technology ecosystem.
- **At least $10 million in annual security software revenue.**
  This Green Quadrant is intended to assess the most prominent vendors offering integrated smart building security software solutions. Although smaller firms may have capabilities similar to those of their larger counterparts, without stronger organizational or financial resources, our research finds that they often cannot truly support an enterprise-wide, multi-site solution. The vendors included in this Green Quadrant study have at least $10 million in annual security software revenue, indicating that they are capable of hiring additional staff to support their solution to meet the needs of diverse customers for the foreseeable future.

Based on the inclusion criteria above, this report evaluated security software solutions from the following providers: Bosch, Brivo, Everbridge, Genetec, Honeywell, Johnson Controls (JCI), LenelS2 (Carrier), Motorola Solutions, Schneider Electric and Siemens (see **Figure 5**). Verdantix invited other vendors to participate, but these firms either failed to respond or declined due to organizational constraints. Eight of the software suppliers included in this study participated in briefings and product demonstrations and provided responses to a detailed questionnaire. Two firms that declined to actively participate were researched based on publicly available information.

Figure 5

Suppliers And Software Assessed

Vendor	Security Solution (s)
Bosch	Bosch Access Management System, Bosch Building Integration System, Bosch Access Control Engine, Bosch Video Management System, Visitor Management
Brivo	Brivo Access, Brivo Global View, Brivo Visitor, Brivo Mobile Pass, Brivo Snapshot
Everbridge	Everbridge Smart Security, Everbridge Control Center, Everbridge Mass Notification and Incident Communications, Everbridge Mobile Application
Genetec	Genetec Security Center, Omnicast, Synergis, Maps, Mission Control, ClearID, KiwiVision
Honeywell	Enterprise Buildings Integrator, Honeywell Digital Video Manager, Honeywell Command and Control Suite, Honeywell Security Manager, Incident Workflow, EBI Reception Manager, Easy Mobile, Edge Security Analytics
Johnson Controls (JCI)	C·CURE, OpenBlue Unified Command Center, C·CURE IQ, C·CURE Visitor Management, C·CURE Go, OpenBlue Active Responder, OpenBlue Secure, victor VideoEdge
LenelS2 (Carrier)	OnGuard, Magic Monitor, S2 (NetBox, NetVR), Elements, OnGuard Visitor
Motorola Solutions	Avigilon Control Center, Access Control Manager, Ava Security (Avigilon Alta), Openpath (Avigilon Alta), ACC Mobile, Compass Decision Management
Schneider Electric	EcoStruxure Security Expert, EcoStruxure Access Expert, EcoStruxure Building Operation, Security Expert Visitor Management
Siemens	Building X Security Manager, Building X Siveillance Add-Ons, SiPass Integrated, SIPORT, Siveillance Control, Siveillance Video, Siveillance Identity, Siveillance Intrusion

Source: Verdantix analysis

Evaluation Criteria

The Verdantix Green Quadrant considers the evolution of the market and customer requirements. We determined our evaluation criteria for this study through a combination of inputs, encompassing interviews with security professionals, desk research, discussions with customers, surveys, and staff expertise.

This inaugural study provides a detailed assessment of 10 prominent integrated security software providers and their product offerings. The analysis included a 113-point vendor questionnaire covering 11 primary categories of capabilities and nine primary categories of market momentum; three-hour live vendor briefings and product demonstrations incorporating specific usage scenarios; bench research; and market interviews. The resulting evaluation is based on the proprietary Verdantix Green Quadrant methodology, which is designed to provide an evidence-based, objective assessment of vendors offering comparable products or services. In our evaluation:

- **Capabilities measure the breadth and depth of functionality.**
  The capabilities dimension, plotted on the vertical axis of the Green Quadrant graphic, measures each provider based on the breadth and depth of its product, its differentiators against other providers, and its proven experience in each area. To assess performance along this dimension, we collected data on 72 detailed criteria across eleven key areas: 1) centralized security management; 2) physical access control management; 3) visitor management and occupant experience; 4) surveillance management; 5) event and alarm management; 6) integration capabilities; 7) data management and business intelligence; 8) development tools; 9) security and privacy; 10) product architecture; and 11) user interface and solution usability.
- **Momentum measures strategic success factors.**
  The momentum dimension of the analysis, as captured on the horizontal axis of the Green Quadrant graphic, measures each provider based on its market and product vision, traction in the market, partnerships, and resources. Evidence was provided by the firms and through Verdantix research. To assess performance along this dimension, we collected data on 41 criteria across nine key areas: 1) market vision and business strategy; 2) product strategy; 3) partner ecosystem; 4) customer base; 5) financial resources; 6) organizational resources; 7) commercial model; 8) deal scope and structure; and 9) geographic reach.

Verdantix weighted each primary criterion and sub-criterion based on its importance within the individual capabilities and momentum dimensions. **Figures 6** and **7** provide details on the study criteria, with the weighting of each primary criterion shown in parentheses. The weightings reflect, among other priorities, the importance for organizations to address security in a holistic, integrated manner. Notably, our Green Quadrant methodology allows for the exploration of vendor standings based on alternative weighting scenarios.

Verdantix defined success measures for each sub-criterion and scored each vendor's performance against these measures on a scale of zero to three. The vendors included in this study are top tier providers and this benchmark evaluates them on a par with one another. As the inaugural Green Quadrant study for this market, we took a conservative scoring approach. The comprehensive nature of this market view, combined with our sub- and primary criteria weightings, influence these vendor standings. Subsequent studies may include a different mix of offerings and weightings and could elicit different results. See **Figures 8** and **9** for the scoring of the integrated security software vendors against the criteria and **Figure 10** for the Green Quadrant graphic summarizing their overall positioning.

Figure 6

Capabilities Criteria For Integrated Smart Building Security Software

Momentum	Questions
Centralized Security Management (16%)	What functionality is provided to support centralized security management activities, such as tools required by global security operation centers (GSOCs)? What security functions and workflows can be acted on from a centralized portal versus through discrete security solution modules? Can and how does the system support multi-site coverage? What centralized security functions can be remotely managed? What centralized security functions are offered as mobile app(s)? What specific role-based functions and capabilities exist for centralized security management and the overall platform? How are users able to configure organizational and system permissions and hierarchy for activities and data access across the platform? Is there specific functionality or out-of-the-box workflows to support the needs of security professionals, guards and front desk personnel; corporate executives and building owners; third-party security services providers and facilities management outsourcers; building occupants and employees; or particular industries? What type of embedded analytical capabilities does the system use to aid centralized security management functions? Does the platform utilize AI or ML tools/capabilities?
Physical Access Control Management (12%)	What functionality is provided to manage physical access control? In what ways does access control integrate for identification and authentication? What credentialling and authentication methods are supported? What type of systems are supported, such as pin pads, biometrics, swipe and smart cards, and mobile devices? What functionality exists for creating and managing traditional tokens and smart badges, such as encoding, printing and decommissioning? To what degree does access control integrate with building security and business management systems such as active directories, video surveillance, alarm management, visitor management, and time and attendance applications? To what degree does the access control software interface with building systems to control building assets in real time (e.g. doors, windows, elevators, turnstiles, intercoms) with entry, stop entry or change access parameters? What capabilities does your solution provide to recognize the building has been breached or access control mechanisms have been tampered? What type of embedded analytical capabilities does the system use to aid in access control management tasks?
Visitor Management & Occupant Experience (4%)	What functionality is provided to address visitor management? Is visitor management integrated with badging, work order systems, wayfinding or other systems? What capabilities exist to monitor and manage parking spaces? What functionality is provided for monitoring and tracking occupant health and wellbeing, including safety concerns such as COVID-19? What functionality is offered for managing contractor information (e.g. credentialling , including prequalification checks, certifications of insurance, financial audits)? What kind of document management capabilities are included in the solution? What type of embedded analytical capabilities does the system use to aid in visitor management tasks?
Surveillance Management (12%)	What functionality is provided for video surveillance? How do you support event and scheduled recordings? How does the video surveillance system integrate with other systems? What functionality is provided for audio surveillance? What functionality exists to monitor assets and equipment in real time to avoid theft or vandalism? What functionality is provided for personal safety monitoring, such as accident detection? What functionality is provided for video and audio content management? How is content history, archival and retrieval for analysis of events managed? What type of embedded analytical capabilities does the system use to aid in surveillance tasks? Does the platform utilize AI or ML tools/capabilities?
Event & Alarm Management (12%)	What functionality is provided to diagnose and manage critical events? What tools are provided to support incident response, such as lockdown and evacuation features? What functionality is provided to create workflows for notifications? What functionality is provided to address intruder alarm management? What functionality is provided for fire and safety alarm management (e.g. fire, CO_2, flood, weather)? What functionality is provided to integrate alarm or event management functions with indoor and outdoor positioning systems? Does functionality exist to send out notifications to occupants based on their location? Does the system automatically support any particular emergency support services and standards? Does the system integrate with regional dispatch services? What type of embedded analytical capabilities does the system use to aid in event and alarm management tasks? Does the platform utilize AI or ML tools/capabilities?

Figure 6 (continued) ↓

Figure 6 (continued)

Integration Capabilities (12%)	What methods are used to support integration with other solutions, such as APIs and prebuilt connectors? What specific standards are supported? What functionality is provided to integrate with building management systems (BMS)? Can and how does the system integrate directly with security hardware and controls versus via a BMS? What types of physical security system hardware and controls manufacturers does your system integrate with and which are automatically supported out of the box? What functionality is provided to capture data or integrate operationally with other building equipment such as elevators, lighting, HVAC? How does the system work with sensor devices and IoT data? What functionality is provided to integrate with third-party workplace, real estate, and facilities management systems, such as IWMS, CMMS, CAD, BIM, and energy management solutions? What functionality is provided to integrate with other enterprise systems, such as ERP, finance, HR, EHS, or project management applications? What functionality is provided to integrate with communications and collaboration systems such as email, MS Teams, or Slack? What tools are provided to ingest or share data with external sources (e.g. weather forecasts local/regional emergency alerts, news feeds)?
Data Management & Business Intelligence (5%)	Does the system provide its own BI tooling or is it sold with a third-party BI tool? What capabilities exist to report, extract and analyse historical data? Does the system contain prebuilt reports and metrics? How can a customer create new or modify existing reports? How can a customer export data to build their own analytics or import into their own BI tool? What data discovery tools are available? What are the systems archiving capabilities and processes for retrieval for analyses in a security event? What dashboarding and visualization tools are available? What functionality is provided for users to view, chart and analyse data? Can users create and customize dashboards themselves (without requiring managed services)? Are role-based dashboards available out of the box? Are tools provided to build security operations performance and optimization models, forecasts, or simulations, such as AI/ML frameworks or toolkits, geospatial capabilities or digital twin functionality? What database technologies does the solution use? How does the platform handle unstructured data? What are the database performance details? How readily can data be stored on the cloud or on-premise, and are there any use cases supported for edge data processing?
Development Tools (5%)	What kind of development tooling is provided? Does the vendor provide a traditional development environment or low-code/no-code capabilities? What development tools can clients use to create new or customize applications or system modules? Is there functionality for users to change or add business rules or workflows, and if so, how? Does the solution have a separate or integrated business rule engine or workflow engine? To what degree can the application and system be modified? What elements can be readily configured? Does the vendor provide capabilities for users to version, package and promote their own solution changes (e.g. development, testing, production)?
Security & Privacy (5%)	What is the vendor's approach to securing applications, data and systems? Are all data encrypted and to what degree? What protocols and support does the system provide to ensure privacy? What types of security certifications and attestations has the vendor or solution achieved, such as ISO 27001/27002, GSA, HIPAA, or SOC? How does the software support customers' regulatory and compliance requirements, such as GDPR? How does the solution address system access rights? To what extent can users configure permissions? Can customers integrate access rights with other systems? What vulnerability assessments are performed on the system? Are third-party vendors used to perform cyber security audits; and if so, which firms are being used and how often? Are penetration tests run and if so, how often?
Product Architecture (5%)	How many different product architectures and code bases does the solution contain? What architectures and development languages are used? What implementation options are available (i.e, cloud, on-premise, multi-tenant, single-tenant)? Is the solution hosted in dedicated data centres or on public cloud services? Does the offering support edge computing and if so, how? What types of connectivity does the solution support? Does the solution provide capabilities to monitor the health of connectivity with other systems and devices? What is the vendor's SLA for data recovery? How does the vendor manage new technical product/service releases?
User Interface & Solution Usability (12%)	How do users engage with the solution? Is there a primary portal? Is there a common interface and navigation protocol used across all security application functions or are there separate interfaces? What is the usability and user-friendliness of the application, web, mobile and alternative interfaces? Does the system support varied types of screen real estate, including wide screens and display walls? Can the system support 2D and 3D geospatial rendering? How many user languages are provided out of the box? Can the software manage multiple time zones?

Source: Verdantix analysis

Figure 7

Momentum Criteria For Integrated Smart Building Security Software

Momentum	Questions
Market Vision & Business Strategy (15%)	What is the vendor's overall market vision for addressing security? What problems is the vendor trying to solve and for what types of users (e.g. specific roles or functions, industries, firm sizes, geographies)? How does the firm intend to achieve its market vision? What market opportunities has the vendor pursued in the past and what does it seek to address over the next three years? What is the firm's vision for the evolution of customer requirements over the next three years? What specific value propositions is the vendor bringing to the security marketplace? What is the firm's business strategy to meet the needs of its target customers over the next three years?
Product Strategy (18%)	What is the vendor's overall security product strategy for the next two-three years? What is the vendor's two-three-year product development roadmap? What new functions, use cases or industries is the vendor looking to serve and how is it planning to achieve these (e.g. through acquisitions, integrations, in-house development)? How can the different solutions the vendor is offering be applied – together or separately – in client situations? Does the firms have a strategy for supporting converged physical, cyber, social, and event-based security?
Partner Ecosystem (15%)	With which, and with how many, services firms does the vendor have formal relationships (i.e. development and Implementation firms, security services, smart building consultancies)? With which, and with how many, software and IT hardware providers does the vendor have a formal relationship, beyond integration? With which, and with how many, building and security-specific equipment firms does the vendor have a formal relationship? With which data and content providers does the vendor have a formal relationship, beyond integration? Does the firm have any co-development arrangements?
Customer Base (16%)	What is the total number of firms using the vendor's building security software? What number of sites are using the vendor's building security software? What is the vendor's customer retention rate in the most recent reporting year? What is the distribution of customers across the security solution module? What is the percentage of customer use by deployment type, such as on-premise and cloud? In which building types is the solution implemented (e.g. corporate real estate, stadiums, hospitals, educational campuses)? How long do most implementations take? How customized do customers tend to make their implementations? What percentage of implementations require services partners?
Financial Resources (10%)	What is the vendor's R&D strategy? What percentage of revenue does the firm invest in R&D? What were the firm's revenues from building security software in the past 12 months or last annual reporting period? By how much did the vendor's total building security software revenues grow in the past year? What is the typical size(s) of the firms' security solution customers? What are the firm's top industries for its security solution? In which industries has the vendor experienced the most growth in revenues over the past two years?
Organizational Resources (8%)	How many employees does the vendor dedicate to its security software business? How many employees are dedicated to its security services and support business? What does the vendor do to support ongoing adoption and user engagement? Does the vendor offer security solution training and certification programmes? Does the vendor run customer success programmes associated with its security solutions? In which countries does the vendor have an office that supports building security solutions?
Commercial Model (5%)	How does the vendor charge customers for use of its security solutions? What licensing model(s) are used (e.g. per user, per module) and are there any add-on options and charges? How does the vendor structure and protect data access and ownership of customer data during and after a formal business relationship has ended? Does the vendor charge customers for any services related to the development or implementation of its security solutions? What types of services and charging model(s) does the vendor apply? Does the vendor charge for any other type of technology or services related to building security (e.g. hardware, content, security audits, security surveillance services)?
Deal Scope & Structure (5%)	What was the vendor's average security software deal size, including all subscriptions and perpetual licence fees over the past year? How many security software deals did the vendor sign over the past 12 months? What was the distribution of deals by solution module? What percentage of the vendor's customers are on an annual, quarterly or monthly contract? What is the average contract length (in years) for subscription deals signed?
Geographic Reach (8%)	What percentage of the vendor's customers are headquartered in North America, Europe, Asia-Pacific and the Rest of the World?

Source: Verdantix survey

Figure 8

Vendor Capability Scores

	Bosch	Brivo	Everbridge	Genetec	Honeywell	Johnson Controls	LenelS2 (Carrier)	Motorola Solutions	Schneider Electric	Siemens
Centralized Security Management	1.4	1.3	2.0	2.2	1.8	2.0	1.7	1.8	1.3	2.3
Physical Access Control Management	1.9	1.8	0.7	2.2	1.8	2.3	2.3	2.3	2.0	2.2
Visitor Management & Occupant Experience	1.6	1.0	0.3	1.4	1.9	1.8	1.7	0.6	1.3	1.5
Surveillance Management	2.2	0.9	0.8	2.5	2.0	1.5	1.1	2.6	0.8	1.6
Event & Alarm Management	1.4	1.0	2.4	2.1	2.1	1.5	1.0	1.0	1.5	2.6
Integration Capabilities	1.3	1.3	2.1	1.9	1.9	1.8	1.5	1.3	1.4	1.6
Data Management & Business Intelligence	1.0	1.9	2.1	1.6	1.7	2.1	1.0	1.4	1.4	1.9
Development Tools	1.0	0.3	2.6	2.6	1.9	1.6	1.0	1.9	1.0	1.9
Security & Privacy	1.4	1.3	2.0	2.7	1.5	1.9	1.7	1.8	1.7	1.5
Product Architecture	1.4	1.5	1.9	2.1	1.8	1.9	1.7	1.3	1.5	1.8
User Interface & Solution Usability	1.2	1.9	2.5	1.3	1.6	2.0	1.9	2.1	1.2	2.0

Vendor provides evidence of market-leading functionality, supported by a broad set of references to customer examples	3
Vendor provides evidence of strong functionality, supported by a broad set of references to customer examples	2
Vendor provides evidence of moderate functionality, with limited references to customer examples	1
No response provided or publicly available, or supplier has a weak offering	0

Source: Verdantix survey

Figure 9

Vendor Momentum Scores

	Bosch	Brivo	Everbridge	Genetec	Honeywell	Johnson Controls	LenelS2 (Carrier)	Motorola Solutions	Schneider Electric	Siemens
Market Vision & Business Strategy	1.0	2.3	2.0	1.3	1.4	1.4	1.0	1.3	1.4	2.4
Product Strategy	0.7	2.0	1.6	1.5	2.2	2.6	0.9	0.9	1.0	2.3
Partner Ecosystem	1.0	2.2	1.5	1.7	1.2	2.0	2.2	1.6	1.1	0.7
Customer Base	1.2	2.5	1.7	2.2	1.3	2.5	2.1	1.7	1.6	2.2
Financial Resources	1.0	1.8	0.9	2.5	1.4	2.0	1.3	2.6	1.2	1.6
Organizational Resources	1.9	1.5	1.8	2.1	1.8	2.8	1.6	1.6	2.1	2.0
Commercial Model	1.8	1.9	1.2	1.9	1.4	1.2	1.3	1.1	1.9	2.0
Deal Scope & Structure	0.7	2.0	1.3	2.0	1.8	1.8	1.7	1.5	1.2	2.6
Geographic Reach	1.3	0.5	1.0	1.5	1.5	1.3	1.5	1.3	1.5	1.3

Vendor provides evidence of market-leading functionality, supported by a broad set of references to customer examples	3
Vendor provides evidence of strong functionality, supported by a broad set of references to customer examples	2
Vendor provides evidence of moderate functionality, with limited references to customer examples	1
No response provided or publicly available, or supplier has a weak offering	0

Source: Verdantix survey

Figure 10
Green Quadrant For Integrated Smart Building Security Software 2023

Capabilities

This dimension measures each software supplier on the breadth and depth of its software functionality across 11 capability areas, as outlined in **Figure 6** & **Figure 8**.

Momentum

This dimension measures each software supplier on 9 strategic success factors, as outlined in **Figure 7** & **Figure 9**.

Note: A white plot indicates a non-participating vendor.
Source: Verdantix analysis

Honeywell Offers A Flexible Building And Security Platform

Founded in 1906 and headquartered in Charlotte, North Carolina, Honeywell is an industrial and technology conglomerate that operates four primary business groups: Aerospace; Building Technologies; Safety and Productivity Solutions; and Performance Materials and Technologies. Honeywell Building Technologies (HBT) offers digital solutions and products, such as building management systems (BMSs), and fire, electrical and security products, to ensure buildings are safe, sustainable and energy-efficient.

Honeywell's core security solution set encompasses its Command and Control Suite (CCS), its Enterprise Buildings Integrator (EBI), an IP-based Digital Video Manager (DVM) for video and audio surveillance, and Edge Security Analytics. EBI is a modular system that has evolved over more than two decades as an integrated, multi-domain BMS; at its core is a supervisory control and integration platform. EBI can connect to third-party cloud systems and is Internet of Things (IoT)-enabled, able to leverage Honeywell's Forge Cloud and Niagara platform for edge device integration and analytics. CCS is an integrated console and client interface to facilitate operations across multiple systems. It provides dynamic mapping capabilities and, through its Incident Workflow optional solution, processes can be configured to guide users through steps to follow, such as standard operating procedures (SOPs). Honeywell offers its own suite of standard and intelligent video analytics solutions; its DVM can also support third-party offerings. Mobile apps are available for remote operations and occupant access activities. According to Honeywell, EBI can be deployed on-premise or in a private cloud on a client's platform of choice. The firm is continuing to enhance the systems supported through its EBI Elevate public cloud deployment option.

Security Manager, an element of EBI, addresses access control, including cardholder management and intrusion detection, and can interface with proprietary and third-party controllers and devices. Options such as guard tours and visitor management are also available. In addition to Security Manager and DVM, the EBI suite offers a Life Safety Manager module for fire alarm monitoring and management, a Building Manager module for optimizing and reporting on facility operations such as lighting and HVAC conditions, and an Energy Manager module. Not covered directly in this benchmark analysis, but important to mention, are the other integrated commercial security suites that Honeywell sells, such as Pro-Watch, which is primarily targeted at enterprises, and WIN-PAK for small and medium-sized enterprises (SMEs). The firm also produces a line of access controllers, smartcard readers, time and attendance systems, credentialling devices, and cameras.

Honeywell's target audience typically encompasses includes large, complex environments such as airports, stadiums, universities, correctional facilities, hospitals, data centres, industrial sites, smart cities and municipalities, and mixed-use developments. The firm also provides custom integration and implementation services.

Strengths And Differentiators

Based on the Green Quadrant analysis, Verdantix finds that Honeywell has strengths in its:

- **Dynamic command and control centre platform capabilities.**
  Honeywell's CCS provides a variety of display options, from large touchscreens to single operator interfaces. The Command Console is available for use on many different devices. It is optimized for multi-windows and monitoring frames, and leverages Active Windows to dynamically engage the user. The system provides map-driven interfaces, and its automation rules engine can be used to design user and event-based workflows. The platform can also integrate with communication and notification systems.
- **Optimized alarm management.**
  Honeywell's Alarm Management feature allows users to prioritize, acknowledge and consolidate related alarms. If desired, Incident Workflow can guide operators through appropriate actions, trigger notifications and integrate with mustering activities. Optional add-ons include the Alarm Pager solution and a Deadman Timer to ensure operators respond within pre-set parameters. The firm offers a mobile alarm app, Honeywell

Pulse, while Honeywell Instant Alert Plus provides mass notification capabilities. Honeywell sells its own line of fire detection systems and devices, including its Xtralis brand, which can be integrated into the EBI platform.

- **Integration platform that can work with a broad range of systems and devices.**
  EBI is designed as a broad integration platform, able to interface with security-oriented and other facility and safety systems. Honeywell has developed a variety of native integrations and, along with application programming interfaces (APIs), supports multiple protocols, such as BACnet, LonWorks, Modbus, ODBC, ONVIF, OPC and SNMP. The firm cites examples of working with technologies from vendors such as Assa Abloy, HID Global and SALTO for access and door lock controls; IDEMIA for biometrics; Axis Communications and Bosch for cameras; AIIGoVision and Ipsotek for video analytics; and Gallagher for intrusion detection. While Honeywell has optimized its platform to work with its own DVM offering, it can integrate third-party video management systems (VMSs) where required. Honeywell has traditionally supported open access control systems, such as Mercury Security, as well as its own Temaline portfolio; the firm indicates that other integrations can be developed using EBI's integration tools.

Improvement Opportunities

Based on the Green Quadrant analysis, Verdantix finds that Honeywell could improve by:

- **Creating more streamlined access control and device configuration tooling.**
  Honeywell has an opportunity to optimize how users navigate across multiple access control management functions and device configurations. Integrators and administrators often need to add and update data, parameters and connections. The varied tools and steps to traverse could be further streamlined, especially to support users less familiar with the overall system topography and teams with diverse skill levels.
- **Adding more out-of-the box functionality for common environments and user workflows.**
  Honeywell could create templates and standardize more out-of-the-box functionality for typical security workflows and integration scenarios. The firm's current solution is highly flexible; however, many potential customers would benefit from being able to select from sets of standard options which could then be readily customized.
- **Providing additional cloud service options and mobile security application functionality.**
  EBI Elevate is a Honeywell-hosted software-as-a-service (SaaS) option on Microsoft Azure. To date, this offering has primarily focused on supporting core building management views and functions. Ideally, Honeywell would extend its cloud service portfolio and mobile app functionality to deliver further security and access management coverage and greater remote guard and surveillance capabilities.
- **Educating and expanding its services and technology partner ecosystem.**
  Integrators and the enterprise community are more familiar with Honeywell's commercial security lines as, to date, this vendor has primarily taken on the bulk of EBI-oriented projects. Honeywell has a prime opportunity to build out a stronger services channel for all of its security and EBI-based systems. The firm overtly promotes the use of its vast array of products in conjunction with EBI, but could be less insular in its market approach. Honeywell could engage a wider community to create connectors and add-on solutions to support the expanding needs of customers and the broader enterprise market.

Selection Advice For Buyers

Considering all supplier offerings assessed in the Green Quadrant analysis, we believe that Honeywell should be included on shortlists by the following buyers:

- **Organizations in industries that need to integrate safety and facilities operations with security.**
  Entities such as laboratories, hospitals, large industrial firms and retail complexes require seamless security operations and real-time situational awareness to keep their assets, workers and patrons safe. Organizations that operate these and other complex environments must monitor and manage a broad spectrum of systems and devices that could benefit from engaging with a common platform such as EBI to tie together security and facilities management capabilities. Honeywell places significant importance on ensuring scalability, reliability and fault tolerance to support the challenging operational demands of highly sensitive and expansive sites.
- **Firms looking to create a centralized GSOC or standardized multi-SOC environment.**
  Honeywell's CCS and EBI platform lend themselves to organizations who want their employees to engage with a common set of workflows and a standard interface. Workers can benefit from learning to operate a uniform system that supports multiple subsystems and sites. Honeywell's systems are architected to accommodate broad global security operations centre (GSOC) needs.
- **Businesses needing to weave together a highly tailored security solution.**
  EBI is designed to be an extensible integration platform; organizations with unique requirements may benefit from its flexibility. Honeywell also provides implementation services and has a global presence, to support multinationals that may have a mix of central and localized needs.

verdantix

Independent insight and analysis

Our research is a trusted source for some of the largest and most innovative businesses in the world. With over a decade of reports, data and analysis, our subscribers have access to depths of insight that cannot be found elsewhere.

Whether you are implementing a leading-edge technology strategy, or developing the products and value propositions of the future, our analysis will help you futureproof your thinking.

Our expertise

Environment, Health & Safety

ESG & Sustainability

Net Zero & Climate Risk

Operational Excellence

Smart Buildings

Contact

Verdantix Ltd, 18 Hatfields, London
SE1 8DJ, United Kingdom

contact@verdantix.com
@Verdantix

Opportunities at Verdantix

Since 2008, Verdantix has been delivering high-quality research and advice to its clients. If you're interested in joining a world-class team with an unwavering focus on success, apply to join us today. We are delighted to be hiring across all teams and have a variety of opportunities in both London and Boston